

Notice of Allowability

Application No.

10/017,926

Examiner

Eleni A. Shiferaw

Applicant(s)

MARUYAMA ET AL.

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 06/19/2006.
2. ☒ The allowed claim(s) is/are 3,6,9,18,20 and 29.
3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☒ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08),
Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit
of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413),
Paper No./Mail Date _____
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____

NASSER MOAZZAMI
PRIMARY EXAMINER

[Signature]
8/25/06

DETAILED ACTION

1. Claims 3, 4, 6, 9, 18, 20, and 29 have been examined. Examiners amendment has been made for claims 3, 6, 9, 18, 20, and 29, and dependent claim 4 have been canceled based on the telephone interview, with Anne Vachon Dougherty on August 24, 2006.

EXAMINER'S AMENDMENT

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Anne Vachon Dougherty on August 24, 2006.

3. Examiner amends claims 3, 6, 9, 18, 20, and 29, and cancels claim 4.

3 (Currently Amended) A proxy server for relaying communications between applications and for performing an additional process comprising:

a key manager for managing multiple keys used to generate a digital signature to be provided for a message document that is exchanged between said applications, wherein each of said multiple keys is used to sign messages having particular message contents;

a signature key determiner for extracting said message document from a

predetermined application, and for, based on the contents of said message document, determining a selected key from said multiple keys that is to be used to provide a digital signature, wherein said contents do not include any digital signature data; and

a signature generator for providing a digital signature for said message document by using said key selected that is obtained from said key manager based on a determination made by said signature key determiner, and for transmitting said message document with said digital signature to a destination application,

wherein said key manager sets multiple key selection rules ~~for obtaining said key~~, and only when said key selection rules are satisfied can said signature generator obtain said selected key, and wherein, when said selected key for generating a digital signature for said message document can not be obtained, said signature generator employs a predetermined replacement key ~~that is defined in advance~~ to provide a digital signature, and

wherein, after said signature generator has provided a digital signature using said replacement key, when said selection rules are satisfied to enable the acquisition of said selected key, said signature generator again provides a digital signature using said selected key.

4. (Canceled)

6. (Currently Amended) The proxy server according to claim 3 ~~claim 4~~, further comprising a log manager for storing said message document with a digital signature

provided by said signature generator, and for managing a log, and wherein said log manager stores not only said message document for which said signature generator has provided a digital signature using said replacement key, but also said message document without digital signature; and wherein said signature generator obtains, from said log manager, said message document without said digital signature, and provides a digital signature using said selected ~~original~~ key.

9. (currently amended) A digital signature system comprising:

applications for performing data processing; and
a proxy server connected to said applications via a network, wherein said proxy server manages multiple keys,

wherein each of said multiple keys is used to sign messages having particular message contents, and wherein said proxy server intercepts a communication, transmitted through said network, from one of said applications to an external destination device, selects one selected key of said multiple keys based on said message contents, provides a digital signature for a message document exchanged via said communication using said selected key ~~selected based on the contents of said message document~~, wherein said contents do not include any digital signature data, and transmits said message document with said digital signature to said external destination device, and

wherein said proxy server permits a key used to provide a digital signature to be changed in accordance with the contents of a message document; and wherein said

proxy server sets key selection rules ~~for said key~~ and permits digital signature using said selected key when said key selection rules have been satisfied, and

wherein, when said key selection rules ~~for said key used to provide a digital signature for said message document~~ have not been satisfied, said proxy server employs a predetermined replacement key to provide a digital signature; and wherein, when said key selection rules ~~for said key~~ are satisfied after said digital signature has been provided using said replacement key, said proxy server again employs said selected key to provide a digital signature for said message document.

18. (currently Amended) A storage medium ~~on which input means of a computer stores~~ embodying a computer-readable program that ~~permits said~~ causes a computer to perform:

a process for selecting one selected key of a plurality of keys used to provide a digital signature for a message document in accordance with the contents of message document transmitted from a predetermined application, wherein said contents do not include any digital signature data and wherein each of said plurality of keys is used to sign messages having particular message contents;

a process for providing a digital signature for said message document using said selected key ~~that is selected~~, and for employing a predetermined replacement key to provide said digital signature for said message document, when key selection rules ~~for said key used to provide a digital signature for said message document~~ have not been satisfied; and

a process for employing said selected key to provide again a digital signature for said message document, when said key selection rules ~~for said key~~ are satisfied after said digital signature has been provided using said replacement key.

20. (currently amended) A program transmission apparatus comprising:

storage means for storing a program that permits a computer to perform:

a process for selecting one selected key of multiple keys used to provide a digital signature for a message document in accordance with the contents of the message document transmitted from a predetermined application, wherein said contents do not include any digital signature data and wherein each of said multiple keys is used to sign messages having particular message contents;

a process for providing a digital signature for said message document using said selected key ~~that is selected~~ and for employing a predetermined replacement key to provide said digital signature for said message document when key selection rules ~~for said key used to provide a digital signature for said message document~~ have not been satisfied; and

a process for, when said key selection rules ~~for said key~~ are satisfied after said digital signature has been provided using said replacement key, employing said selected key to provide again a digital signature for said message document; and

transmission means for reading said program from said storage means, and for transmitting said program.

29. (currently amended) A computer-implemented digital signature method for providing a digital signature for a message document exchanged by applications and for authorizing said message document, comprising the steps of:

selecting, in accordance with the contents of a message document generated by one of said applications, one selected key of a plurality of keys used for providing a digital signature for said message document, wherein said contents do not include any digital signature data and wherein each of said plurality of keys is used to sign messages having particular message contents;

providing a digital signature for said message document; and

transmitting said message document with said digital signature to a destination designated by said one of said applications, wherein key selection rules are provided ~~for said key~~ and further comprising the steps of:

providing a digital signature for said message document, when key selection rules ~~set for said key~~ are not established, by using a predetermined replacement key ~~that is set in advance for said key~~;

using said selected key, when said key selection rules ~~for said key~~ have been satisfied after said digital signature has been provided using said replacement key, to again provide a digital signature; and

transmitting said message document with said digital signature to said destination.

Allowable Subject Matter

4. The following is an examiner's statement of reasons for allowance:

Claims 3, 6, 9, 18, 20 and 29 are allowed.

Claims 3, 9, 18, 20 and 29: Prior art of record neither alone nor in combination teach a apparatus/system/medium/a program transmission apparatus/method for providing a digital signature for a message document exchanged by applications by using a selected key from plurality of keys, for intercepted messages that do not contain any digital signature data/information, when messages are transmitted over the network, generating a digital signature using the selected key when key selection rules are satisfied, and generating digital signature using a replacement key when key selection rules are not satisfied, and to again provide a digital signature for said message document, when the key selection rules for the key are satisfied after the digital signature has been provided using the replacement key.

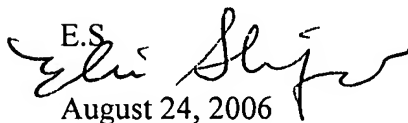
Claim 6 is allowed because of dependency.

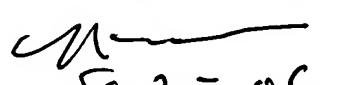
Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

E.S.

August 24, 2006

NASSER MOAZZAMI
PRIMARY EXAMINER

8/25/06